



**HEADQUARTERS
CIVIL AIR PATROL VIRGINIA WING
UNITED STATES AIR FORCE AUXILIARY**
7401 Airfield Drive
Richmond, Virginia 23237-2250



24 February 2003

MEMORANDUM FOR All VIRGINIA WING PERSONNEL

FROM: Headquarters Virginia Wing, Director of Information Technology

SUBJECT: National E-Services Web Security Administrator (WSA) Policy

Recently National Headquarters' E-Services System has undergone some major revisions. These updates have improved the ability to support the assignment of administrative rights to designated personnel below the Wing level. As such we will be delegating the ability for the Groups and Units to manage the restricted access in the National E-Services area for their respective areas of authority.

The following policy is being established to control the implementation and use of the National E-Services System. Instructions on how to use the WSA function are attached to this policy. It is important to note that by giving a member permission to access web applications in E-Services, you are entrusting that member to privileged data. Any tampering that member may do will ultimately be linked back to you (You are their Sponsor).

- 1) As authorized by the Wing Commander, the Wing WSA's will manage all Wing Staff and wing level access to E-Services. Additionally, the Wing WSA's will assign the WSA authorizations to a representative from each Group as authorized by the Group Commander.
- 2) As authorized by the respective Group Commander, the Group WSA will manage all Group Staff and group level access to E-Services. Additionally, the respective Group WSA will assign WSA authorizations to a representative from each Squadron in their Group as authorized by the respective Unit Commander.
- 3) As authorized by the respective Squadron Commander, the Squadron WSA will manage all Squadron Staff access to E-Services for their respective unit.
- 4) Only one WSA per unit below the Wing level should be assigned. Requests for additional WSA's in a unit must be justified and approved by the Commander of the next higher level.
- 5) The Social Security Number Search privilege in the E-Service System will not be assigned to any member without explicit authorization from the Wing Commander.
- 6) The following privileges will not be assigned below the Wing level:
 - a. Form 18, Form 73 and Form 82; all units are required to submit their monthly reports to the Wing as directed by appropriate guidance.
 - b. Calendar Admin, activities and events must be coordinated with the Wing to prevent conflicts.
- 7) The Personnel Information Change function should only be assigned with the approval of the respective Unit Commander. This function while useful to assist those without access to the Internet, it must be used with caution as it has the ability to alter membership information in the National System.

- 8) The Commanders and WSA's for each respective Unit will insure that the system is kept current. Access to restricted functions will be unassigned as soon as it is determined that the member no longer has a requirement to access a particular function.

All transactions performed in the National E-Services System are logged by National Headquarters. The log contains the transaction performed, who performed it and when. Any evidence of misuse will be reported to the Wing Commander for appropriate action.

Questions concerning this policy letter should be directed to Wing Headquarters. Technical problems with the application should be directed to National Headquarters Help Desk. There is a link from the Login Screen of the E-Services application to the Help Desk. It contains additional instructions, FAQ and contact information.

For the Commander,

Mark Kunkowski, Major, CAP
Director, Information Technology

Attachments:

- 1) WSA Instructions

Civil Air Patrol Web Security Administrator Instructions

The Web Security Admin page allows the web security administrator (WSA) (either the commander or his designated representative(s)) to do the following:

- Grant member access to “restricted” web applications located under the Restricted Application section of eServices.
 1. Restricted applications are those usually associated with functional transactions and reports that are available because of a job or specialty requirement. (Examples: updating pilot qualification data, inputting CAPF 73 vehicle monthly summary data, etc)
- Assign web security administrator status to others.
 1. NHQ MSI assigns web security administrator privileges to one member at each region and wing member as designated by the region/wing commander. In addition, NHQ/MSI assigns all permissions to web pages for the NHQ staff and National commander’s staff.
 2. Wing and group web security administrators assign web security administrator privileges for at least one lower echelon member as designated by each of the lower echelon unit commanders.
- All web security administrators grant/remove permissions to the various “specific” web pages as directed by their unit commander.
 1. Permissions may be granted to both unit members and non-unit members that are in the national database.
 2. Permissions granted allow access to information only at the level of the administrator granting the permissions. (Example: permissions granted by a squadron administrator provide access only to information associated with that squadron; permission granted by a group, wing, or region administrator will provide access to information for all units associated with that group, wing, or region)

Allowing a member to access eServices

In order for a member to access the ‘eServices’ section of the CAP website, they must first have a UserID and password. This will automatically be sent to the member once the member's web registration is complete. Non-members must contact NHQ MSI to obtain a UserID and password. The process for members is simple.

1. You will need a valid email address for the member needing access.
2. Go to the [Member Registration page](#).
3. Fill out the member's SSN# and email address.
4. Hit the submit button.
5. Once this button is pressed, the user will receive an email with their User ID and temporary password to access CAP’s eServices section of our website.

If the member does not receive an email within a few days, please contact [NHQ MSI](#) for assistance.

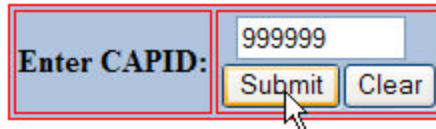
Assigning permissions - Step-By-Step Procedures

The following are systematic procedures for granting and removing permissions once you have logged into eServices and selected the WSA Admin application:

Note: NHQ tracks who assigns and removes each permission.

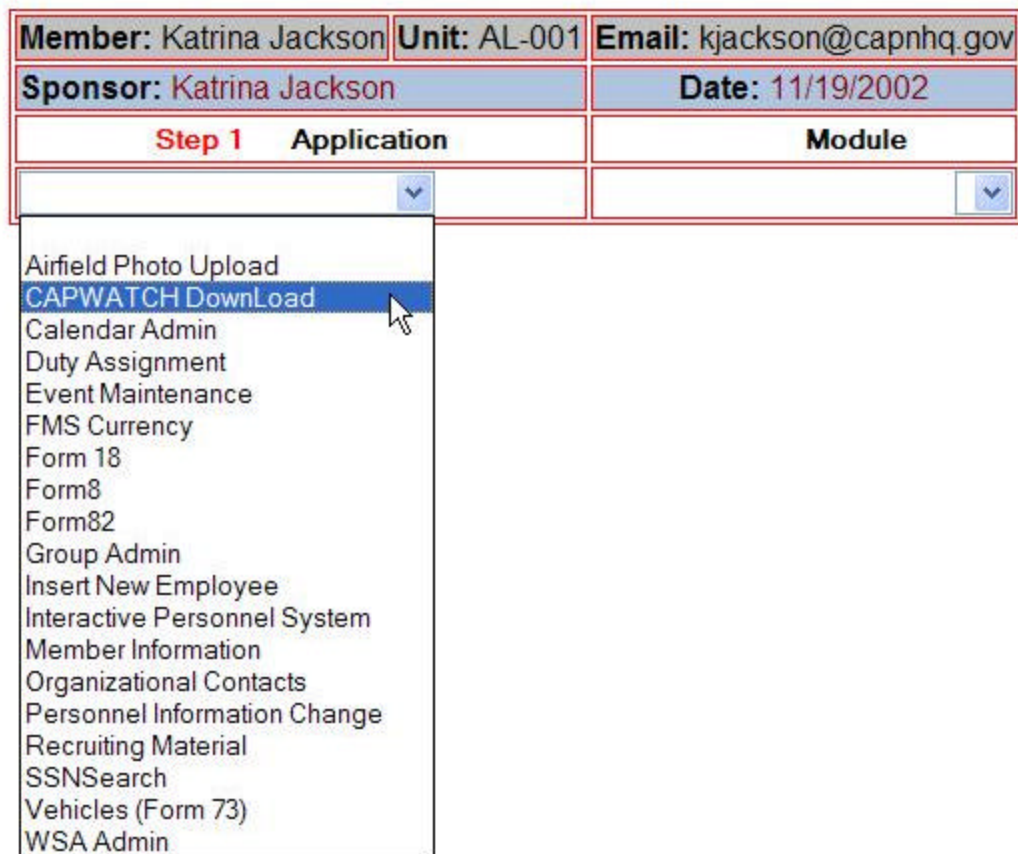
1. When the form loads, you’ll notice a text box for CAPID located on the left side of the screen. Enter the person’s CAPID for which you want to grant permissions (You may also enter your own).

Welcome [Katrina Jackson](#) .If you need a member's CAPID, try the [Interactive Personnel System](#).



2. Upon clicking the 'Submit' button, you will be presented with a new screen on the right. Verify the person's name before continuing to ensure you have entered the correct CAPID. Verify that an email address exists. If not, this person you are trying to give permissions have not registered to use eServices. Follow the above instructions on how to "allow a member to access eServices" prior to assigning permissions. Next, select an application from the dropdown box.

WSA Admin Application



3. Each application will consist of at least one "Module". A module is a specific section of an application. For instance, the **new** application M.I.M.S. (Member Information Management System) may have several modules such as Qual/Cert, Validate Achievements/Tasks, and FMS Currency (These modules use to be known as individual applications). Since each of these modules perform different functions for the overall M.I.M.S. application, each must be assigned individually. If the application only performs one function, the module will usually have the same name as the application. Select the Module you would like to assign permissions.

WSA Admin Application

Member: Katrina Jackson	Unit: AL-001	Email: kjackson@capnhq.gov
Sponsor: Katrina Jackson		Date: 11/19/2002
Application		Step 2 Module
CAPWATCH DownLoad ▼		▼

Description: Allows a user to download CAPWATCH for WSA.

4. The next step involves Processes. A process is an action you can perform within a module. Some common processes include "Read-Only" and "Data-Entry". Previously, this was known as "read" and "write". Each module will have at least one process. You will assign the process by functional area, organization, and scope.
 - **Functional Area** -The application processes can be performed within various functional areas. For example, for the module "Qual/Cert" you may want to give a member Data Entry permissions to OPS-CAPPilot area, but Read-Only permissions to OPS Emergency Services area. Check each functional area that you want to assign for the process. We have included a convenient "Check All" button if you want to assign all of the functional areas.
 - **Organization** - Select the unit you want this process to apply.
 - **Scope** - Scope is an area of permissions. Now you are able to restrict permissions to a certain level or area. For instance, if you have a member that need to see AL-001 data only and not the entire Wing, you will select UNIT for scope instead of WING. (WING scope gives a member access to all of the units within the Wing and REGION Scope gives a member access to all of the wings and units within the Region.) We have added a new scope called MEMBER. You may rarely see this scope available. This scope means the member can only access his or her own record.

WSA Admin Application

Member: Katrina Jackson	Unit: AL-001	Email: kjackson@capnhq.gov
Sponsor: Katrina Jackson		Date: 11/21/2002
Application		Module
M.I.M.S. ▼		Qual/Cert ▼

Step 3:

Process	Functional Area	Organization	Scope
Data Entry	<input checked="" type="checkbox"/> OPS-CAPPilot	Wing: AL ▼ Unit: 001 ▼	UNIT ▼
	<input type="checkbox"/> OPS-Emergency_Services		
Read-Only	<input type="checkbox"/> OPS-CAPPilot	Wing: AL ▼ Unit: 001 ▼	WING ▼
	<input checked="" type="checkbox"/> OPS-Emergency_Services		

5. At any time, you could review a member's permissions by clicking on the [Quick View](#) link. Here, you may also remove permissions by clicking on the "Delete" button. If you would like to remove several permissions at once, click on the [Delete one or more Application \(s\)](#) link. Check each permission you would like to remove and click the "Delete Application(s)" button. A convenient "Check All" button will automatically check each permission

for you. Then you would proceed by clicking on the "Delete Application(s)" button. **Warning:** This will remove all of the permissions selected with no additional confirmation.

NOTE FOR ALL:

1. By giving a member permission to CAP web applications, you are entrusting that member to privileged data. Any tampering that member may do will ultimately be linked back to you (You are their Sponsor).
2. You may only delete web applications that were assigned to that member at your organizational level (your wing or unit) or below (unit in your wing or group).